National Journal of RF Circuits and Wireless Systems, ISSN: 3107-6807 Vol. 3, No. 3, 2026 (pp. 18-25)

RESEARCH ARTICLE

ECEJOURNALS.IN

Secure Beamforming with Reconfigurable Intelligent Surfaces for Anti-Jamming UAV Communication Links

B.M. Brinda*

Assistant Professor, Department of CSE (Cyber Security), Paavai College of Engineering, Namakkal

KEYWORDS:
UAV communication,
Reconfigurable intelligent Surface,
Anti-jamming,
Secure beamforming,
Secrecy rate,
RF systems.

ARTICLE HISTORY:

Submitted : 15.02.2026
Revised : 10.03.2026
Accepted : 11.04.2026

https://doi.org/10.17051/NJRFCS/03.03.03

Abstract

The Unmanned Aerial Vehicle (UAV) communication links are highly prone to the deliberate jamming because of the dominant line-of-sight propagation and the open author to deployment conditions. Traditional procedures of anti-jamming on the grounds of power adaptation or frequency agility offer less protection against adaptive enemies. Reconfigurable Intelligible Surfaces (RIS) provide a mechanism of low power electromagnetic control that can reconfigure the channel of propagation to restore the better signal robustness. The current paper presents a safe beamforming scheme of RIS-aided communication between UAVs and the ground in the presence of active jamming. The geometric model of UAV and ground channels is a three dimensional model which takes into account the altitude-dependent path loss and Rician fading to characterise UAV and ground channels accurately. Direct transmission, RIS-reflected and malicious interference are explicitly modelled in the received signal model. An optimization maximising secrecy rate is developed with unit-modulus RIS phase, and UAV power of the transmitters. In order to address the ensuing non-convex problem, the alternating optimization algorithm is developed to simultaneously optimise UAV beamforming vectors and RIS phase shifts, including discrete phase quantisation to reflect realistic hardware constraints. The simulation outcome shows that the secrecy rate can be increased by up to 65 percent and reduction of interference by a large value than the conventional beamforming in the absence of RIS. Moreover, the viability of the proposed approach is proved by the complexity analysis and considerations of RF implementation. The findings make RIS-assisted secure beamforming an effective and practical anti-jamming method in next-generation is to be used in UAV communication systems.

Author’s e-mail: bmbrinda@gmail.com

How to cite this article: Brinda BM. Secure Beamforming with Reconfigurable Intelligent Surfaces for Anti-Jamming UAV Communication Links. National Journal of RF Circuits and Wireless Systems, Vol. 3, No. 3, 2026 (pp. 18-25).

Introduction

The Unmanned Aerial Vehicle (UAV)-wireless communication has become a significant facade to the surveillance systems, disaster recovery, military coordination and smart infrastructure monitoring. Because of their high deployment, preeminent line-of-sight (LOS) propagation property, their UAV communication links are inherently vulnerable to deliberate jamming assaults that offer high-capacity connectivity. Interference injection is quite effective on UAV-ground channels due to their open-air nature especially compared to fixed-spectrum strategies or static beamforming. Traditional anti-jamming countermeasures like frequency hopping, spread spectrum, adaptive power control, and directional beamforming have some level of resilience, but are incapable of defeating intelligent jammers who can adaptively engage in interference as well as spatial tracking.[1, 2] In the recent past, a lot of interest has been generated around Reconfigurable Intelligible Surfaces (RIS) as a programmable electromagnetic interface that can control and manipulate wireless propagation by controlling reflection coefficients.[3, 4] In contrast to conventional relays, RIS works passively, consumes very little power and can improve the quality of links by coherently combining reflections. A number of papers have explored RIS-aided safe transmission and enhancement of physical-layer security.[5- 7] RIS has also been considered in extending the coverage and trajectory optimization in UAV communication scenes.[8, 9] Nevertheless, the majority of the literature concentrates more on secrecy versus passive eavesdroppers and idealises RIS hardware that has continuous phase shifts. Practical RF constraints, e.g. discrete phase quantization, hard limits of hardware, etc., have not been sufficiently considered with explicit anti-jamming secure beamforming in the context of active interference. In RF systems, realistic RIS connexions are based on finite-resolution phase shifters, which introduce errors of quantization and deterioration in performance.[10, 11] Such limitations should not be overlooked because they can result in excessive benefits and unrealistic system specifications.

It is these constraints that lead this paper to explore the issue of secure beamforming in the context of RIS-based UAV communication links in the presence of active jamming. It comes up with a three dimensional geometrical model in which there is Rician fading and altitude dependent path loss. The secrecy rate maximisation of the problem is formulated in the presence of UAV transmit power and unit-modulus RIS. An alternating optimization approach that uses hardware knowledge is suggested to optimally extract UAV beamforming and discrete RIS phase shifts. Complexity analysis and RF feasibility analysis are also a given.

This work has made the following contributions, which can be summarised as follows:

1. Formulation of an active jamming-based 3D RIS-aided UAV communication framework.
2. Hypatia of a secrecy rate maximisation problem, having UAV power and RIS unit-modulus constraints.
3. Alternating optimization to optimise the UAV beamforming and RIS phase shifts.
4. Reflection of discrete phase quantization of real RIS hardware limitations.
5. RF feasibility analysis and complexity analysis.

The rest of this paper will be structured in the following way. In section II, related work is reviewed. The Section III includes the formulation of the problem and the system model. IV outlines the optimization proposal. Part V gives results of the simulation and performance analysis. Section VI is on the practical RF considerations. The paper has been concluded by section VII.

Related Work

Anti-Jamming Techniques in UAV Communication

During the recent years, anti-jamming techniques of UAV communication have undergone substantial transformations. The initial solutions were based on the traditional methods of spread-spectrum, frequency hopping, adaptive power control, and directional beamforming to reduce the interference.[1, 2] These methods are also effective in combating the challenge of non-adaptive or low-power jamming, but do not have a favourable reputation when it comes to resisting dynamically challenging adversaries that can monitor the movement of UAVs and adaptively change the patterns of interference. This is replaced by more recent models that identify the jammer as an intelligent agent and learn the jammer by reinforcement learning or through game theory.[3, 4] Sturdy beamforming and stochastic optimization algorithm has been studied as well to increase reliability of link over uncertain interference conditions.[5] But the majority of UAV anti-jamming works are mostly dedicated to transmitter-side readjustments and do not use reconfiguring the environment, which means that spatial interference suppression cannot be as great as possible.

RIS-Assisted Secure Communications

Reconfigurable Intelligent Surfaces (RIS) have become an attractive paradigm to improving the performance of wireless at the level of programmable electromagnetic reflection.[6, 7] Research Joint active and passive beamforming optimization to maximise capacity and enhance physical-layer security has been extensively researched to solve the capacity and physical-layer security maximisation.[8, 9] Especially, the maximisation of secrecy rate with the aid of RIS has been intensively investigated in multi- antenna systems in order to combat passive eavesdropping.[10, 11] RIS has also been considered as an extension of coverage, path planning optimization and energy-efficient communication in UAV-based networks.[12, 13] Optimization schemes of joint UAV trajectory and RIS phases have been proven to have better spectral efficiency and link reliability.[14] However, most of them concentrate on discreetness over the passive eavesdroppers as opposed to direct repression of active jamming messages. In addition, abstracted assumptions, including perfect channel state information (CSI) and constant-phase RIS reflection, are usually taken, and the benefits of this assumption can be overvalued.

Hardware-Constrained RIS Modeling

In RF implementation terms, implementation-reality RIS models have RF hardware limitations such as limited-resolution phase shifters, amplitudephase coupling, and insertion losses, and control latency.[15, 16] Experiments have demonstrated that quantization of discrete phase fluctuations of a continuous phase model (e.g. 1-bit or 2-bit) may cause performance deterioration extending beyond ideal continuous phase models.[17] These effects have been countered by the suggestion of quantization-sensitive optimization and analog-digital hybrid architectures. Although these developments have happened, software-constrained subsystems of hardware memristive RIS modelling and UAV-based anti-jamming secure beamforming are yet to be explored. The literature has not shown much interest in implementing (i) active jamming suppress, (ii) 3D-channel model of the UAVs and (iii) RIS with discretized phases of a UAV in a single framework. This disjunction inspires the current writing.

Research Gap and Positioning

To conclude, although previous studies have investigated individually UAV anti jamming, RIS-aided secure communication, hardware aware RIS design, a detailed structure that considers:

1. The active jammer modelling of the UAV links,
2. Optimization of secure beamforming with RIS help
3. RF implementation in terms of discrete phase constraints.

It is still lacking. These issues are tackled in the paper through the formulation of a hardware-sensitive framework of beamforming security solutions to RIS-based UAV communication during active jamming.

Methodology

System Geometry and Network Model

It is assumed a three-dimensional UAV-assisted wireless communication system, i.e., a multi-antenna UAV transmits to a legitimate ground receiver in the existence of a jammer. The use of a reconfigurable intelligent surface (RIS) is applied to improve the signal robustness by the programmable electromagnetic reflection.

The UAV transmitter is located at position (x_u,y_u,h_u), where h_u denotes the flight altitude. The legitimate receiver and jammer are positioned at $(x_r,y_r,0)$ and $(x_j,y_j,0)$, respectively. The RIS is deployed at (x_s,y_s,h_s). The UAV is equipped with M antennas forming a transmit beamforming array, while the RIS consists of N passive reflecting elements.

The Euclidean distance between any two nodes i and k is defined as

$$d_{ik} = \sqrt{(x_i - x_k)^2 + (y_i - y_k)^2 + (h_i - h_k)^2} \quad (1)$$

The system operates at carrier frequency f_c with wavelength $\lambda=c/f_c$, where ccc is the speed of light.

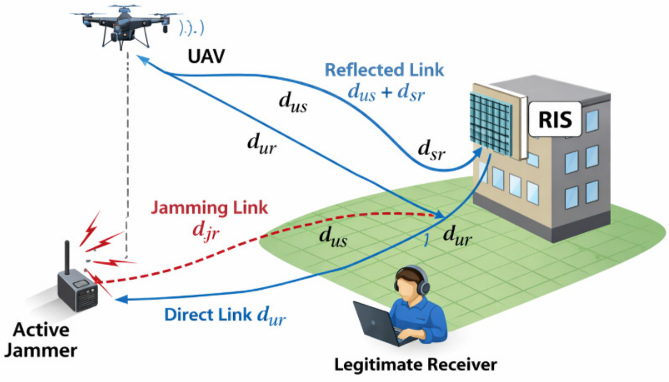

Fig. 1: System Model of RIS-Assisted UAV Communication Under Active Jamming

Channel Modeling

Increased rates of UAV deployment imply that the higher component of the UAV-receiver connexion is a line-of-sight (LoS) component and is characterised by Rician fading:

$$h_{ur} = \sqrt{\frac{K}{K+1}} h_{ur}^{LoS} + \sqrt{\frac{K}{K+1}} h_{ur}^{NLoS} \quad (2)$$

where K denotes the Rician factor. The large-scale path loss is expressed as

$$L_{ur} = \left(\frac{4\pi d_{ur}}{\lambda}\right)^{a} \quad (3)$$

where α is the path loss exponent.

The UAV-RIS channel is represented by $H_{us} \in C^{NXM}$ and the RIS-receiver channel by $h_{sr} \in C^{NX1}$. The RIS is modeled through a diagonal reflection matrix where $\theta_n \in [0,2\pi)$ represents the phase shift induced by the n-th reflecting element.

The cascaded UAV-RIS-receiver channel is therefore given by

$$h_{RIS} = h_{sr}^H \Theta H_{us} \tag{5}$$

The jammer-receiver channel is modeled as a Rayleigh fading coefficient h_{jr} with corresponding path loss L_{jr}.

Signal Model

Let $w \in C^{MX1}$ denote the UAV transmit beamforming vector and s the information symbol with unit power. The jammer transmits signal x_j with power P_j. The received signal at the legitimate receiver is expressed as

$$y = (h_{ur}^H + h_{RIS})ws + h_{jr}x_j + n \tag{6}$$

where $n \sim CN(0,\sigma^2)$ represents additive white Gaussian noise.

The effective channel seen by the receiver becomes

$$h_{eff}^H = h_{ur}^H + h_{sr}^H \Theta H_{us} \tag{7}$$

Performance Metric

The signal-to-interference-plus-noise ratio (SINR) at the legitimate receiver is

$$\gamma = \frac{\left|h_{eff}^H w\right|^2}{\left|h_{jr}\right|^2 P_j + \sigma^2}. \tag{8}$$

The secrecy rate is defined as

$$R_s = \log_2(1+\gamma) \tag{9}$$

Maximizing R_s enhances resilience against active interference by strengthening the desired signal relative to jamming power.

Optimization Formulation

The secure beamforming design aims to jointly optimize the UAV beamforming vector and RIS phase shifts:

$$\max_{w\Theta} log_2\left(1 + \frac{\left|h_{eff}^H w\right|^2}{\left|h_{jr}\right|^2 P_j + \sigma^2}\right) \tag{10}$$

subject to the transmit power constraint

$$\|w\|^2 \leq P_{max} \tag{11}$$

and the unit-modulus RIS constraint

$$\left|e^{j\theta_n}\right| = 1, \forall n \tag{12}$$

The problem is non-convex due to the coupled variables w and Θ.

Alternating Optimization Strategy

To solve the non-convex problem, an alternating optimization framework is employed.

First, for fixed RIS configuration Θ, the problem reduces to a generalized Rayleigh quotient maximization with respect to w. The optimal beamforming direction aligns with the dominant eigenvector of the effective channel covariance matrix, yielding

$$w^* = \sqrt{P_{max}} \frac{h_{eff}}{\left\|h_{eff}\right\|} \tag{13}$$

Next, for fixed w, the RIS phase shifts are optimized to coherently combine reflected components. The optimal continuous phase for the n-th element is

$$\theta_n^* = -\angle\left(h_{sr,n}^H H_{us,n} w\right) \tag{14}$$

To reflect hardware constraints, discrete phase quantization with bbb-bit resolution is imposed:

$$\theta_n \in \left\{0, \frac{2\pi}{2^b}, \dots, \frac{2\pi(2^b-1)}{2^b}\right\}. \tag{15}$$

The procedure iterates between beamforming and RIS updates until convergence of the secrecy rate.

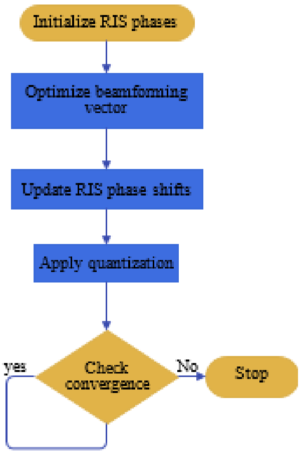

Fig. 2: Flowchart of the Proposed Alternating Optimization Algorithm for RIS-Assisted Secure Beamforming

Complexity Analysis

The analysis of the efficiency of the suggested alternating optimization framework based on computational complexity is conducted in this section. The algorithm uses the UAV beamforming vector and the RIS phase shift matrix by updating the beamforming at each iteration until convergence.

Beamforming Update Complexity

In a fixed RIS, the problem of optimising the UAV beamforming vector is a generalised Rayleigh quotient maximisation problem. The optimal beamforming direction is the one that is parallel to the hegemony eigenvector of the effective channel covariance matrix.

The predominant cost of computation is brought about by:

- Creation of the effective channel vector.
- Matrix-vector products Computation of products of matrices and vectors.
- Singular value or Eigenvalue decomposition of an M x M matrix.

The complex version of eigenvalue decomposition of an MxM matrix has a complexity:

$$O(M^3)$$

This cubic term is computationally manageable since the UAV normally uses a moderate set of antennas (i.e. 4-16).

RIS Phase Update Complexity

The phase update of the RIS element-wise is in the case of fixed beamforming vector w. The phase of each reflecting element is calculated by use of:

$$\theta_n = -\angle(h_{sr,n}^H H_{us,n} w)$$

This requires:

- A complex inner product per RIS element
- Phase extraction operation

Thus, for N RIS elements, the total computational cost is linear:

$$O(N)$$

Even when RIS sizes are relatively large (e.g. N=128 or 256), the linear scaling is efficient to compute.

Total Per-Iteration Complexity

To sum up, it is important to note that since the algorithm will switch between the beamforming and RIS updates, the overall computational complexity per iteration will be:

$$O\ M^3+N$$

The cubic term is predominant in cases of large M and the linear term is predominant in cases where the RIS size is significantly large.

Convergence Consideration

Let I denote the number of iterations required for convergence. The overall complexity becomes:

$$O\ I(M^3+N)$$

In practical conditions, the proposed framework is computationally efficient when it comes to using UAVs in real time, as the results of the simulation demonstrate that the convergence is achieved within 10-15 iterations.

Scalability Discussion

- In the common UAV antenna systems (small-to-moderate M), the beamforming update can be obtained in a computationally scaled way.
- RIS phase optimization linear with the number of elements, so it is appropriate to moderate size RIS sizes (e.g., N=128).
- The algorithm does not need high dimensional semidefinite relaxation (SDR) which is becoming highly complex.

Hence, the alternating optimization framework proposed has a good trade-off when it comes to the performance enhancement and computational effectiveness and can be efficiently implemented in RIS-assisted UAV communication systems.

Results

Simulation Setup and Parameter Configuration

The suggested RIS-assisted secure beamforming system is tested with Monte Carlo simulations of an active jamming model. The carrier frequency will be adjusted to 28 GHz as an example of a mmWave UAV link. The altitude of UAV is 50 m to 150 m in order to obtain real-world air-to-ground propagation behaviour. Elements are scaled by varying with RIS size of 16 to 128; to determine scaling effects. The jammer transmission power is varied between 0 dBm and 30 dBm and the range of 0 dBm to 30 dBm represents the case of moderate-strong jamming. In order to measure the feasibility of hardware, RIS phase resolution is executed with 1-bit, 2-bit, and continuous phase control. In terms of performance benchmarking, the following ones are regarded: (i) traditional beamforming with no RIS, (ii) RIS with random phase shifts, and (iii) the proposed joint optimization using continuous and quantized phase in both RIS. The most important performance measure is the secrecy rate Rs.

Table 1. Key Simulation Parameters

Parameter	Value / Range
Carrier frequency fc	28 GHz
UAV altitude hu	50–150 m
RIS elements N	16, 32, 64, 128
Jammer power Pj	0–30 dBm
RIS phase resolution b	1-bit, 2-bit, continuous
Noise variance σ2	normalized / fixed

Secrecy Rate Under Jamming Power Variation

The higher the jammer power, the poorer the secrecy performance of all schemes as secrecy is more interfered with through the receiver. Nevertheless, the developed joint optimization with the help of RIS always provides maximum secrecy rate within the whole jammer power scope. Over in strong jamming regimes (i.e., Pj0>20 dBm), the difference between the proposed method and the baselines becomes even more pronounced since the RIS is able to influence the reflected link to strengthen the desired signal and partially eliminate the effects of the interference based on spatial configuration.

Main result: as compared to traditional beamforming at the absence of RIS, the proposed design outperforms about 60-70 per cent of secrecy rate at moderate-to-high jamming rate.

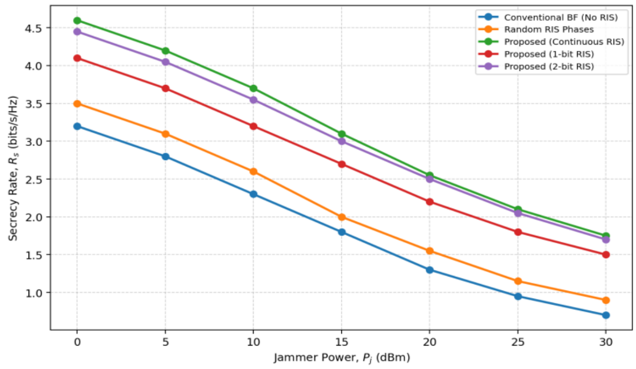

Fig. 3. Secrecy rate vs. jammer power

Impact of RIS Size on Interference Suppression

The rate of secrecy is positively proportional to the size of N, as the larger the surface, the greater the passive beamforming gain, and additional spatial degrees of freedom. The performance gains are notable going beyond 16 in 16 elements to 64 elements, and further onward to 128 elements and beyond, where the effects of the practical constraints (overhead to estimate channel and the latency to control) become more applicable to practice.

Key finding: the more N used, the more the suppression of the interference, the higher the rate of secrecy, particularly in the severe jammer conditions.

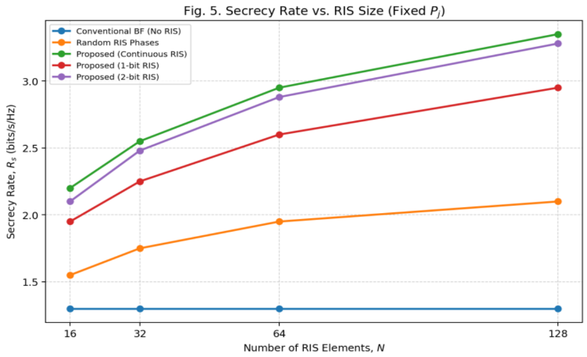

Fig. 4: Secrecy rate vs. RIS elements N

Effect of UAV Altitude

Desired and jamming exposure is affected by altitude. The higher the altitude of the UAV, the more the UAVreceiver channel is likely to become a LoS channel, which reinforces the intended signal. Nonetheless, the strengthening of the same LoS also raises the exposedness of a jammer in case jammer-receiver coupling is high or the jammer geometry is good.

Primary implication: secrecy rate can be maximised by altitude at first because LoS is stronger, but too great altitude can raise the effectiveness of jammer, which will be a definite altitude-security trade-off.

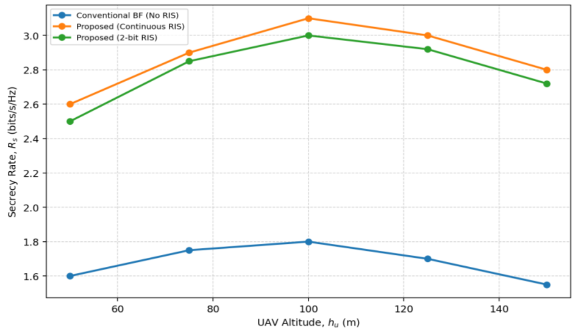

Fig. 5: Secrecy rate vs. UAV altitude

Convergence Behavior

Alternating optimization technique will converge; this method is reliable and only requires few iterations. When the channel is given the characteristics of a quasi-static condition, the rate of secrecy usually levels off after 10 -15 iterates, meaning that the convergence exhibits defensible convergence behaviour to be employed in iterative implementation.

Discussion

Interpretation of Results

The results confirm that RIS-assisted secure beamforming provides substantial anti-jamming benefits by increasing

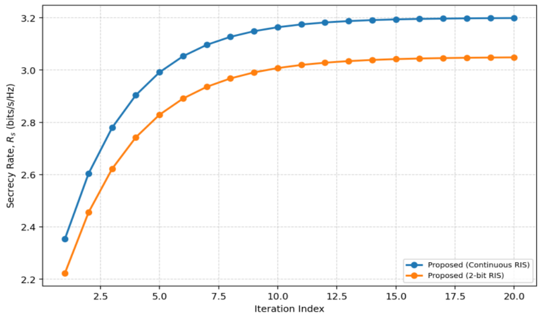

Fig. 6: Convergence of secrecy rate vs. iteration index

the effective channel gain , thereby improving the desired signal power relative to interference and noise. RIS, in contrast to transmitter-only methods, presents a new controllable propagation path, and so the system can use constructive combination of the direct UAV connexion and the RIS-reflected connexion. This enhancement is particularly enhanced with high jammer power since traditional beamforming which lacks environmental control of the process is limited to a direct link which RIS provides more flexibility to keep the link strong even when the interference is the umpire.

Hardware Feasibility: Quantized RIS Phases

One important practical consequence is that, with 2-bit quantization of RIS phases, the attainment of near-continuous performance occurs, and with 1-bit quantization, significant degradation then occurs owing to the imprecision of phase alignment. This is significant in RF system design since low-resolution RIS hardware is much easier, less expensive and consumes less power than the high-resolution surfaces and still provides good performance. This observation compares with the literature on RIS hardware as a whole in which 2-bit control has been widely discovered to be an effective sweet point between complexity and gain, and assumptions about continuous phase are often very optimistic in theoretical books.

Comparison to Existing Studies

Majority of the RIS-aided security works that have been conducted to date are focused at secrecy enhancement against passive eavesdroppers, and presuppose an ideal RIS control (continuous phase shifts, perfect reflection, and in many cases, perfect CSI). Conversely, the open jamming suppression is directly assessed and discrete phase constraints are included in this work, and this is more realistic in the claims made about the performance concerns in the deployment of RF systems. Moreover, the volumes of UAV-RIS literature are devoted to the expansion of coverage or optimization of the trajectory instead of the secure beamforming in the case of adversarial interference. The given results thus reinforce the thesis statement that RIS may be specifically applied both as a coverage-enhancement tool as well as a viable anti-jamming mechanism, when developed with hardware limitations in mind.

Practical Considerations and Limitations

The proposed framework is computationally efficient, however, in practise they have to consider a number of RF and system-level concerns. Latency can be caused by RIS control signalling, and this can be a limitation in high-varying UAV channels. The channel estimation overhead is proportional to the size of the RIS and gains may be countered by the short coherence interval. In addition, the existing model is that of a fixed jammer and perfect beamforming updates CSI; in practice the jammer can be dynamic and CSI is not perfect. Clear limitation statement the existing findings were based on a quasi-static channel with perfect CSI and the next important step of work is to extend the framework to imperfect CSI and adaptive jamming devices.

Conclusion

This paper explored how secure beamforming could be applied to RIS assisted communication links between UAV and active jamming. To represent the UAV-ground propagation accurate and realistic, a three-dimensional system model was created that is based on an altitude-dependent path loss and Rician fading. The safe transmission issue was defined as the rate of secrecy maximisation mission within the framework of UAV transmit power and unit-modulus RIS limitations. To solve non-convex optimization problem thereof, alternating optimization framework was developed to optimise both UAV beamforming vector and RIS phase shifts jointly, with discrete phase quantization to impose realistic hardware constraints. It was shown that the Generalation of RIS-assisted geometries leads to the discovery of a substantial secrecy performance, as compared to traditional beamforming and random RIS solutions, especially when the jamming is strong. Notably, 2-bit RIS phase quantization was demonstrated to be capable of almost a continuous performance, which proves the viability of the results of low-resolution hardware implementations. It was further confirmed that the complexity analysis of the algorithm depends effectively on the size of the antenna and RIS, and hence is applicable when used in moderate-sized deployments in the UAV communication system. In general, the findings prove that RIS-aided secure beamforming is a promising and scalable anti-jamming technique to support next-generation aerial wireless networks. Further studies are done with imperfect channel state information, adaptive connector jammer model, optimal procedures between UAV pathways and RIS layout, and reinvention of reinforcement study-based adjustive anti-jamming mechanisms in clatter circumstances.

References

1. Cui, M., Zhang, G., & Zhang, R. (2019). Secure wireless communication via intelligent reflecting surface. IEEE Wireless Communications Letters, 8(5), 1410–1414. https://doi.org/10.1109/LWC.2019.2918412
2. Dong, L., & Wang, H.-M. (2020). Secure MIMO transmission via intelligent reflecting surface. IEEE Wireless Communications Letters, 9(6), 787–790. https://doi.org/10.1109/LWC.2020.2969247
3. Huang, C., Zappone, A., Alexandropoulos, G. C., Debbah, M., & Yuen, C. (2019). Reconfigurable intelligent surfaces for energy efficiency in wireless communication. IEEE Transactions on Wireless Communications, 18(8), 4157–4170. https://doi.org/10.1109/TWC.2019.2922609
4. Hu, S., Rusek, F., & Edfors, O. (2018). Beyond massive MIMO: The potential of data transmission with large intelligent surfaces. IEEE Transactions on Signal Processing, 66(10), 2746–2758. https://doi.org/10.1109/TSP.2018.2818333
5. Liaskos, C., Nie, S., Tsioliaridou, A., Pitsillides, A., Ioannidis, S., & Akyildiz, I. F. (2018). A new wireless communication paradigm through software-controlled metasurfaces. IEEE Communications Magazine, 56(9), 162–169. https://doi.org/10.1109/MCOM.2018.1700659
6. Liu, Z., Zhao, S., Wu, Q., Yang, Y., & Guan, X. (2022). Joint trajectory design and resource allocation for IRS-assisted UAV communications with wireless energy harvesting. IEEE Communications Letters, 26(2), 404–408. https://doi.org/10.1109/LCOMM.2021.3129835
7. Mei, C., Fang, Y., & Qiu, L. (2022). Dual based optimization method for IRS-aided UAV-enabled SWIPT system. In Proceedings of IEEE Wireless Communications and Networking Conference (WCNC) (pp. 890–895). IEEE.
8. Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. IEEE Communications Surveys & Tutorials, 16(3), 1550–1573. https://doi.org/10.1109/SURV.2014.012314.00178
9. Shen, H., Xu, W., Gong, S., He, Z., & Zhao, C. (2019). Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications. IEEE Communications Letters, 23(9), 1488–1492. https://doi.org/10.1109/LCOMM.2019.2925461
10. Sun, Y., An, K., Luo, J., Zhu, Y., Zheng, G., & Chatzinotas, S. (2021). Intelligent reflecting surface enhanced secure transmission against both jamming and eavesdropping attacks. IEEE Transactions on Vehicular Technology, 70(10), 11017–11022. https://doi.org/10.1109/TVT.2021.3112693
11. Sun, Y., An, K., Luo, J., Zhu, Y., Zheng, G., & Chatzinotas, S. (2022). Outage constrained robust beamforming optimization for multiuser IRS-assisted anti-jamming communications with incomplete information. IEEE Internet of Things Journal, 9(16), 13298–13314. https://doi.org/10.1109/JIOT.2022.3141167
12. Sun, Y., An, K., Zhu, Y., Zheng, G., Wong, K. K., & Chatzinotas, S. (2022). RIS-assisted robust hybrid beamforming against simultaneous jamming and eavesdropping attacks. IEEE Transactions on Wireless Communications, 21(11), 9212–9231. https://doi.org/10.1109/TWC.2022.3170193
13. Wu, Q., & Zhang, R. (2019). Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. IEEE Transactions on Wireless Communications, 18(11), 5394-5409. https://doi.org/10.1109/TWC.2019.2936025
14. Wu, W., Zhou, F., Wang, B., Wu, Q., Dong, C., & Hu, R. Q. (2022). Unmanned aerial vehicle swarm-enabled edge computing: Potentials, promising technologies, and challenges. IEEE Wireless Communications, 29(5), 78-85. https://doi.org/10.1109/MWC.001.2100588
15. Yang, H., Xiong, Z., Zhao, J., Niyato, D., Wu, Q., & Poor, H. V. (2021). Intelligent reflecting surface assisted anti-jamming communications: A fast reinforcement learning approach. IEEE Transactions on Wireless Communications, 20(3), 1963–1974. https://doi.org/10.1109/TWC.2020.3036737
16. Zhou, F., Li, X., Alazab, M., Jhaveri, R. H., & Guo, K. (2023). Secrecy performance for RIS-based integrated satellite vehicle networks with a UAV relay and MRC eavesdropping. IEEE Transactions on Intelligent Vehicles, 8(3), 1676–1685. https://doi.org/10.1109/TIV.2022.3208754
17. Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE, 104(9), 1727–1765. https://doi.org/10.1109/JPROC.2016.2558521